景, 对系统进行大量性能测试. 测试显示, 在一台八核主频 2.8 GHz 8 GB 的安卓设备上, 通过私钥解密信息的平均时耗为 23 毫秒; 将生成身份二维码的平均时耗为 52 毫秒; 在一台四核 3.3 GHz 8 GB 服务器上, 收到获取链上数据平均时耗为 130 毫秒, 在数据量上升至 20 万条后, 获取链上数据平均时耗为 470 毫秒, 其中测试结果主要受用户移动设备性能、服务器性能和网络延迟影响, 系统功能的可用性、信息验证的有效性、数据交互的正确性、生物认证的准确性都满足业务分析中提到的要求.

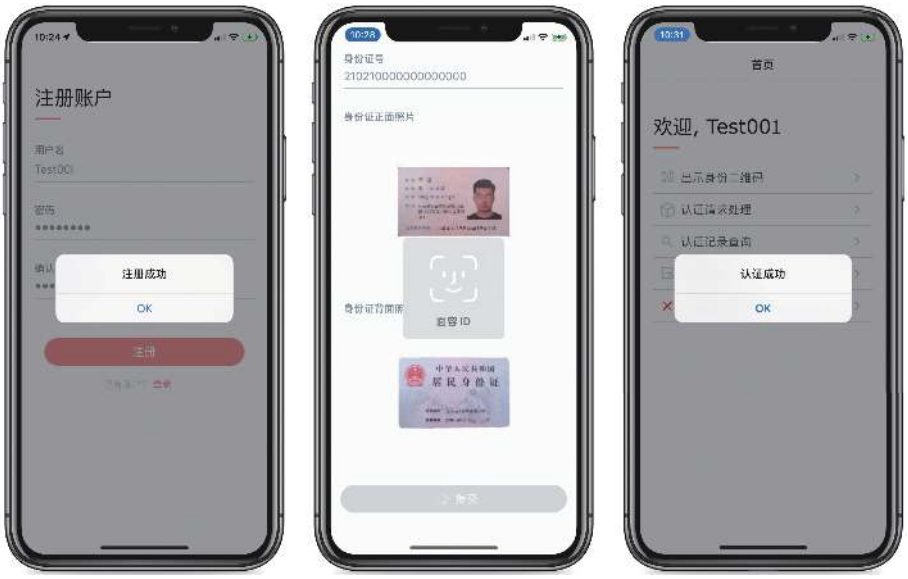

图 10 身份信息提交

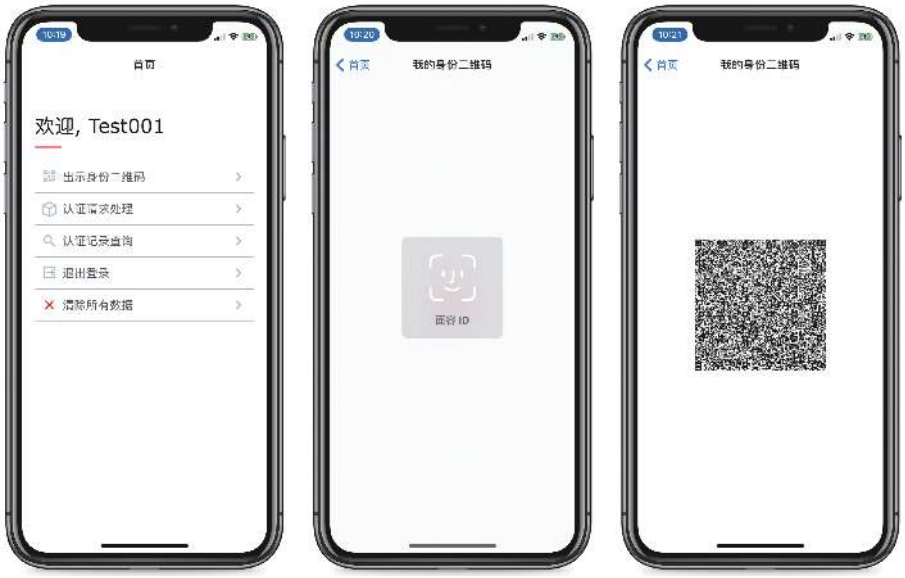

图 11 身份二维码

4 结论

为了推进铁路旅客身份认证管理由集中式向去中心或多中心化创新发展, 优化铁路旅客身份认证管理的运作流程, 本文面向智能手机用户端, 设计并实现了一套基于区块链应用模式的铁路旅客身份认证管理系统. 第一, 系统把旅客身份信息保存在客户端本地, 信

息摘要封存在链上, 实现了铁路旅客身份信息本地存储、链上校验, 验证时无需出示明文身份信息, 仅需出示存有相关信息的数据摘要、公钥的二维码即可, 校验方通过寻址对比就能验证信息真实性, 有效避免了铁路旅客身份信息泄露问题. 第二, 系统将旅客身份信息数据分布式存储, 采用时间戳技术增强了旅客身份数据的抗篡改性和可追溯性, 利用非对称加密技术在保护旅客隐私、实现实名制的前提下增强了数据的透明性、安全性和鲁棒性, 进行生物信息认证确保了铁路旅客对身份信息的所有权, 部署智能合约提高了铁路旅客身份认证的准确性和智能化水平, 提供 API 实现第三方认证集成调用, 提供 SDK 实现二次扩展集成开发.

本研究的局限表现在没有对生物识别技术进行独立开发, 而是采取调用智能手机用户端自带生物识别接口的方式, 实现生物识别的功能. 下一步的研究可以考虑面向服务端来搭建私有链并对区块数据存储与智能合约的进行深入开发研究.

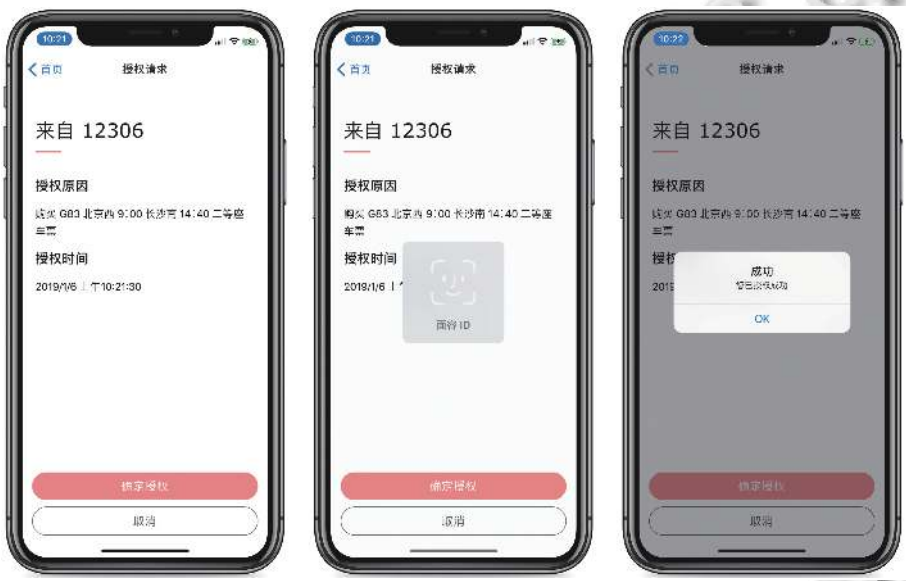

图 12 认证请求处理

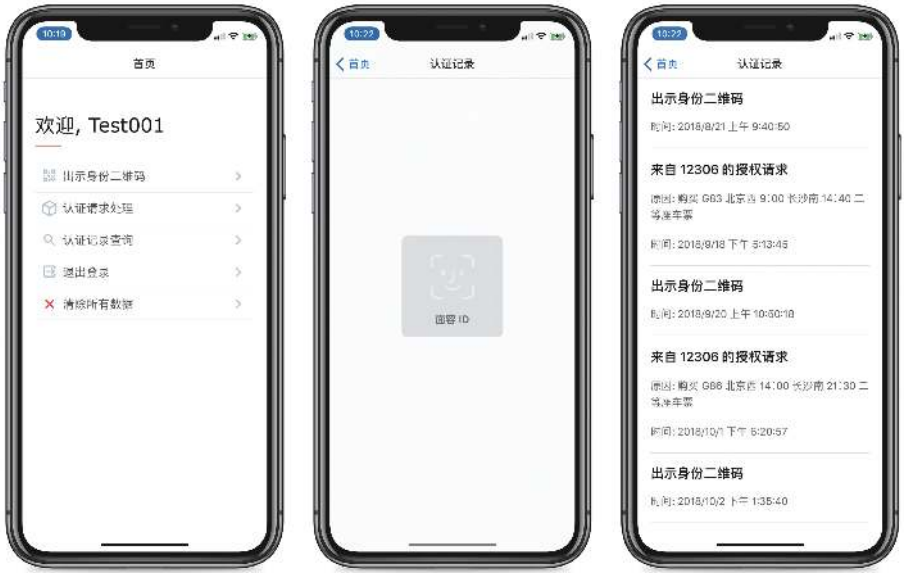

图 13 认证记录查询

参考文献

1 Swan M. Blockchain thinking: The brain as a decentralized autonomous corporation. IEEE Technology and Society Magazine, 2015, 34(4): 41–52. [doi: 10.1109/MTS.2015.2494358]

2 Swan M. Blockchain temporality: Smart contract time specifiability with blocktime. Proceedings of the 10th International Symposium on Rules Technologies. Research, Tools, and Applications. Stony Brook, NY, USA. 2016. 184–196.

3 Fu DQ, Fang LR. Blockchain-based trusted computing in social network. Proceedings of the 2nd IEEE International Conference on Computer and Communications. Chengdu, China. 2016. 19–22.

4 Sullivan C, Burger E. E-residency and blockchain. Computer Law & Security Review, 2017, 33(4): 470–481.

5 Muzammal M, Qu Q, Nasrulin B. Renovating blockchain with distributed databases: An open source system. Future Generation Computer Systems, 2019, 90: 105–117. [doi: 10.1016/j.future.2018.07.042]

6 Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. Proceedings of 2015 IEEE Security and Privacy Workshops. San Jose, CA, USA. 2015. 180–184.

7 Dunphy P, Petitcolas FAP. A first look at identity management schemes on the blockchain. IEEE Security & Privacy, 2018, 16(4): 20–29.

8 Faísca JG, Rogado JQ. Decentralized semantic identity. Proceedings of the 12th International Conference on Semantic Systems. Leipzig, Germany. 2016. 177–180.

9 吕婧淑, 操晓春, 杨培. 基于区块链和人脸识别的双因子身份认证模型. 应用科学学报, 2019, 37(2): 164–178.

10 王成. 基于区块链的保险业务流程优化方法研究. 铁道运输与经济, 2018, 40(10): 61–65.

11 周亮瑾, 王富章. 铁路客运私有链共识机制关键技术研究. 铁道运输与经济, 2018, 40(6): 59–63.

12 陈宇翔, 张兆雷, 卓见, 等. 基于区块链的身份管理研究. 信息技术与网络安全, 2018, 37(7): 22–26.

13 董贵山, 陈宇翔, 张兆雷, 等. 基于区块链的身份管理认证研究. 计算机科学, 2018, 45(11): 52–59. [doi: 10.11896/j.issn.1002-137X.2018.11.006]

14 彭永勇, 张晓韬. 基于区块链应用模式的可信身份认证关键技术研究. 网络安全技术与应用, 2018, (2): 36–37.

15 王成, 史天运. 区块链技术综述及铁路应用展望. 中国铁路, 2017, (9): 91–98. [doi: 10.3969/j.issn.1007-9971.2017.09.017]

16 黄俊飞, 刘杰. 区块链技术研究综述. 北京邮电大学学报, 2018, 41(2): 1–8. [doi: 10.3969/j.issn.1008-7729.2018.02.001]

17 Brito H, Gomes G, Santos e Jorge Bernardino Á. JavaScript in mobile applications: React native vs ionic vs NativeScript vs native development. Proceedings of the 13th Iberian Conference on Information Systems and Technologies. Caceres, Spain. 2018. 1–6.

18 刘红超, 缪燕, 郝悍勇, 等. 基于代理重加密的 PostgreSQL 系统访问控制方法. 计算机工程, 2018, 44(8): 192–198.